COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 WEST TEMPLE STREET
493 HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

TELEPHONE: (213) 974-2008
FACSIMILE: (213) 633-4733

September 11, 2002

To: Supervisor Zev Yaroslavsky, Chairman
Supervisor Yvonne Brathwaite Burke, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
Chief Information Officer

COUNTY SECURITY ACTION PLAN UPDATE – CYBER-TERRORISM TASK FORCE

This letter is to update you on the County's efforts to date for improving its information security infrastructure to mitigate exposure and to improve response to cyber-incidents. The following accomplishments are attributable to the concerted and dedicated work of many contributing departments.

Following the tragedy that occurred one year ago, September 11, 2001, the Chief Administrative Office (CAO) developed a Security Action Plan in response to a September 25, 2001 Board Order. A Security Action Plan Committee was formed with representatives from numerous departments. The Committee identified and quantified critical action plan priorities and needs. Four sub-groups were immediately formed, including a cyber-terrorism group. Chaired by the Chief Information Office, the Cyber-Terrorism Task Force was initially charged with the "purchase [of] anti-virus software to protect and/or identify, track and isolate terrorism viruses [and/or malicious code] on the County's data systems and secure the County's network." With collaboration from many departments and corporate business partners, the Cyber-Terrorism Task Force quickly identified action plans and strategies addressing the areas of computer incident response, network strengthening and segment isolation, enterprise licensing for anti-virus software, remote access, remote backup and recovery, good operating principles, and security policies and procedures. The Task Force reported its findings to the Security Action Plan Committee, CAO, I/T Board Deputies, Department Heads, and Department Information Technology Managers. Among its accomplishments, the Task Force developed the vision and strategy for creating a new and significant security structure within the County.

The County's new information security organization (depicted in the figure attached) is tasked with establishing and overseeing countywide standards, policies, procedures, and guidelines related to information technology security. An Information Security Steering Committee (ISSC) has been formed, whose purpose is to be the administrative vehicle for overseeing countywide security and planned security initiatives. ISSC members are the departmental chief information security officers (DCISO) and it will be chaired by the County's Chief Information Security Officer (CISO), once appointed.

There are several specialized teams under ISSC that are made up of members from different County departments. The Security Policies team, lead by the Sheriff's Department and with participation from 16 departments, continues to meet regularly to draft countywide policies. The group has identified a total of 13 policies to be developed, three of which (Countywide Master Information Security Policy, Use of County Information Technology Resources by County Employees, Internet Usage Security Policy) have already been completed and provided to the ISSC members for review, prior to final circulation and submission to your Board for adoption.

Also in operation are the Countywide Computer Emergency Response Team (CCERT) and the Security Engineering Team (SET), both lead by the Internal Services Department (ISD) with representation from numerous departments. CCERT communicates security information, identifies and mitigates security risks, and coordinates responses to security incidents across County departments. Through its monthly meetings, CCERT is developing a computer emergency response procedure, a "list server" to aid in the dissemination of threat and response information, an interactive voice response (IVR) system to provide automated information about threats, and a countywide cyber-terrorism Intranet website. The website will contain general information for all County employees, as well as restricted information for CCERT and SET members.

SET focuses on technology and infrastructure related issues. It is comprised of various technical workgroups that will research and develop security solutions for different technology areas. These workgroups meet regularly, with agendas that currently span: evaluating and selecting intrusion detection systems for deployment in the County's network; developing security templates for strengthening servers and network devices; planning a new countywide network re-addressing scheme; designing secure wireless networks; and improving remote access into the County environment.

In addition, enterprise agreements have been established with both of the County's primary anti-virus vendors, Network Associates, Inc. and Symantec Corporation. The agreements cover products for both the desktop and server environments, and include professional services and priority vendor support. Furthermore, a countywide Security Threat Notification Policy has been put into effect to improve and expedite the communication of credible security risks (virus alerts, network intrusions, internal security breaches, etc.) to all computer

users. And, ISD Data Security is maintaining a Computer Virus Hotline at (562) 940-3335 to help disseminate important information.

My office is also proceeding with the appointment of the County's Chief Information Security Officer (CISO), the Chief Information Privacy Officer (CIPO), and an Information Security Specialist. All three are expected to be hired within 45 days.

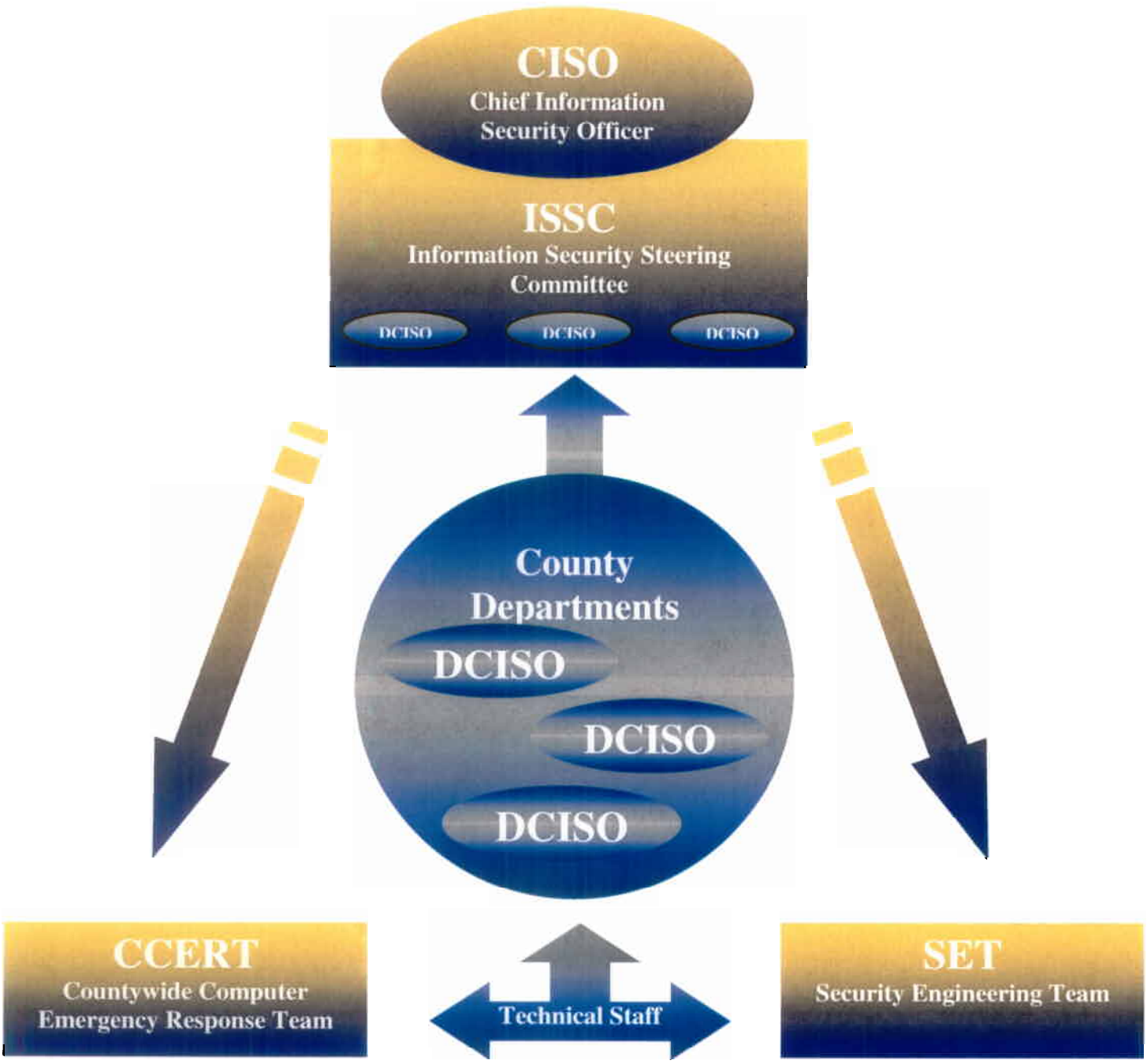
These collective efforts are focused on instituting an enterprise-approach to enhancing the County's ability to mitigate and respond to cyber-attacks. Much has been accomplished as a result of the admirable support and dedication among the departments. Is the County's security posture better than it was a year ago? Absolutely. Is there still much more that can be done? Definitely. But, our security achievements can only be made stronger through the enduring active involvement of all departments. Information security is a vital activity for the entire organization that must be ongoing; security is like breathing – if you stop, you're in trouble. My office will continue to provide coordination and guidance for the County's collaborative information security program.

Should you have any questions, please call me at (213) 974-2008.

JWF:DH:ygd

c: I/T Board Deputies
Department Heads
Department I/T Managers
Information Security Steering Committee
Information Systems Commission

P:\Drafts\Board Security Update 09-11-02.DOC



Los Angeles County Information Security Organization